PSIM – МАРКЕТИНГ И РЕАЛЬНОСТЬ

Рыбаков Михаил Иванович
компания «Итриум»

На сегодняшний день повсеместно – в Интернете, печатных публикациях и презентациях – используется аббревиатура PSIM. Производители программных средств для комплексных систем безопасности активно используют акроним PSIM для продвижения своих продуктов. При этом они часто заявляют о принципиальной новизне и качественном отличии своих средств от всего того, что было ранее.

Возникает резонный вопрос: действительно ли PSIM определяет новый класс систем? А если так, то правомерно ли относить такие средства к этому классу?

ЧТО ТАКОЕ PSIM?

Само понятие PSIM – Physical Security Information Management – возникло где-то в районе 2006 года. К тому времени интегрированные и комплексные системы безопасности (далее КСБ) создавались в России уже как минимум лет десять. Организационно-техническая архитектура КСБ с 1990-х годов была и остается достаточно универсальной *(рис. 1)*.

На верхнем уровне – компьютеры, серверы, программные средства и сетевая инфраструктура. Функциональные контроллеры и панели – это средний уровень. Нижний – оконечные устройства (обобщенно, сенсоры и исполнительные устройства).

Исторически все технические средства, собирающие, обрабатывающие данные и информацию от оконечных устройств, классифицировались как средства/система сбора и обработки информации, т. е. ССОИ. Но с конца 1990-х понятие ССОИ, как правило, адресовано именно верхнему уровню: компьютерам, сетевой инфраструктуре и программным средствам. Таким образом, ССОИ – это система/подсистема верхнего уровня КСБ.

В российской нормативной базе есть определения основных терминов.

ГОСТ РФ 52860-2007. Технические средства физической защиты (ТСФЗ):

Рис. 1. Типовая организационно-техническая архитектура КСБ

КОМПЛЕКСНЫЕ СИСТЕМЫ

«5.4.1. **ССОИ** предназначена для приема, обработки, отображения и регистрации информации, поступающей от СО (средства охраны), а также для формирования команд управления и контроля работоспособности ТСФЗ».

ГОСТ Р 53195.1-2008. Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 1. Основные положения:

«3.11. **Комплексная система безопасности; КСБ:** Система безопасности, одновременно выполняющая несколько функций безопасности, снижающих риски, обусловленные несколькими видами и/или источниками опасностей».

Итак, программные средства ССОИ обеспечивают сбор информации от всех подсистем КСБ, единое управление и реагирование. Подобный класс программных средств был также определен и в ГОСТ Р 52551-2006 как «система интегрированная» и «система интегрированная открытая». Впрочем, необязательно «прислоняться» к регламентированным определениям. Любые проекты и решения КСБ включали подобную функциональность с 1990-х годов, хотя ГОСТ, посвященные КСБ и интегрированным системам безопасности, начали появляться лишь в середине нулевых.

Так может быть, PSIM это ССОИ? Отличаются ли они чем-нибудь?

Обратимся к определению. Аббревиатура PSIM изначально адресована классу программных средств, которые предоставляют платформу для интеграции разных функциональных приложений и технических средств безопасности, а также для управления ими через единый пользовательский интерфейс.

Пока звучит очень похоже на ССОИ. Двигаемся дальше.

Выделяют **6 основных функций систем класса PSIM:**

- **Сбор данных.** Программные средства собирают данные от разнородных устройств, систем безопасности и прочих источников.
- **Верификация.** Программные средства предоставляют разностороннюю информацию о событиях в интуитивно понятном интерфейсе и удобной форме для проверки и подтверждения или отклонения.
- **Анализ.** Программные средства автоматически анализируют, объединяют и сопоставляют прямые и косвенные данные о событиях, состояниях технических средств и сигналах тревог для выявления реальных ситуаций, предупреждения, обнаружения и определения приоритетов реагирования.
- **Поддержка бизнес-процессов.** Программные средства автоматизируют стандартные операционные процедуры (SOP), предоставляя пошаговые инструкции на основе рекомендаций, политики организации и т. н. «лучших практик», а также инструменты для разрешения ситуации.
- **Отчеты.** Программные средства отслеживают и накапливают всю поступающую информацию и информацию о действиях, решениях и командах, содержат встроенные средства построения разносторонних адаптивных отчетов для анализа, проведения тренингов и учебы.
- **Контрольный журнал.** Программные средства отслеживают и регистрируют все действия операторов, принимаемые ими решения, управленческие команды, голосовые переговоры и пр., а также фиксируют время реакции на события и принятия решений.

Сбор данных, верификация событий, контроль действий, инструкции операторам, подготовка отчетов – вся эта функциональность, в том или ином виде, представлена в различных программных средствах и реализована во множестве КСБ. Но появляются два новых свойства – автоматический анализ данных и поддержка бизнес-процессов. Таким образом, общая направленность и дух концепции принципиально отличаются от традиционных требований и нормативных документов, касающихся ССОИ и интеграции.

Во-первых, концепция PSIM – это «управление через информацию» (Information Management). Это более не традиционная «охранная полицейская» система, базирующаяся на опыте, интуиции и бумажном документообороте, а система, функционирующая на основе автоматического анализа данных и инструментов поддержки принятия решений. Основа «управления через информацию» – автоматизированный анализ данных. Разнообразие систем и средств безопасности – СКУД, цифровые системы видеонаблюдения, видеоаналитика, биометрические системы и так далее – порождает огромные объемы информации, которые можно и нужно регистрировать, накапливать и автоматически анализировать для получения качественно нового уровня знаний о безопасности на объекте. Это то, что сегодня называется «Большие данные» (Big data), где применяются технологии Data Mining.

Во-вторых, в PSIM акценты перенесены с управления техническими средствами и системами КСБ на процессы управления безопасностью. Теперь это не просто реагирование, а действия на основе и в соответствии с автоматизированными стандартными процедурами. Как при обработке инцидентов, так и в повседневной деятельности.

Таким образом, концепция PSIM декларирует новый подход к управлению безопасностью и новые требования к программным средствам ССОИ. В этой связи, оправдано применение словосочетаний «программные средства класса PSIM» и подобных.

Важная особенность концепции PSIM – универсальность. Physical Security – это про СКУД, охранную сигнализацию и видеонаблюдение. Но все базовые функции и принципы построения этого класса систем подходят для любых задач сбора, обработки данных, принятия решений и управления. Потому неудивительно, что словосочетание «решение класса PSIM» все чаще распространяют на любые системы: автоматизации зданий, жизнеобеспечения, ситуационные центры и системы «Безопасного города». Одно из наиболее известных подобных решений – концепция «Actionable Intelligence» от компании Verint.

ИНЦИДЕНТНОЕ УПРАВЛЕНИЕ ИЛИ УПРАВЛЕНИЕ ЧЕРЕЗ ИНФОРМАЦИЮ?

Акроним PSIM может ввести в заблуждение. Может возникнуть желание расшифровать PSIM как Physical Security Incident Management (вместо Information Management). Тем самым сводя PSIM к инцидентному управлению вместо настоящего информационного менеджмента.

Стоит отметить, что значения слов INCIDENT и ИНЦИДЕНТ отличаются в английском и русском языках. ИНЦИДЕНТ в русском языке несет однозначно отрицательный смысл чрезвычайной ситуации. В английском же это может быть как чрезвычайная ситуация, авария, так и просто рядовое событие, явление. Потоки событий КСБ в основном не являются проявлениями ИНЦИДЕНТОВ в нашем понимании. Но это не значит, что такие события не имеют значимого отношения к безопасности. Например, данные мониторинга технического состояния системы объекта, статистика сбоев, нарушений регламентов, информация о действиях операторов, выполняемых работах по обслуживанию и ремонту и т. д. – вся эта информация не относятся к ИНЦИДЕНТАМ, но имеет прямое отношение к обеспечению «боевой готовности» систем, профилактике и предупреждению потенциальных тревожных ситуаций.

Таким образом, и процедуры управления в кризисных ситуациях, ИНЦИДЕНТНОЕ управление – есть лишь особые режимы функционирования систем класса PSIM, подмножество процессов общего информационного менеджмента. Но производители программных

средств безопасности при обращении к PSIM делают акцент именно на управлении ИНЦИДЕНТАМИ, а не информацией. Почему? Потому, что управление через информацию – это сложно.

ИНФОРМАЦИОННЫЙ МЕНЕДЖМЕНТ – ЭТО СЛОЖНО

Сегодня в российской практике комплексной безопасности инцидентная (реактивная) направленность является доминирующей. Функции «управления инцидентами» понятны и легко ложатся на существовавшие ранее концепции ССОИ. На «обработке инцидентов», стандартных процедурах и документообороте «карточек инцидентов» основана деятельность ПЦН (пунктов централизованного наблюдения). В более масштабных реализациях КСБ эти же принципы сегодня внедряются как «решения класса PSIM».

Есть, по крайней мере, два объективных фактора, которые затрудняют переход от «инцидентной модели» к информационному управлению безопасностью. Это низкая доступность данных для интеллектуального анализа и отсутствие разработанных моделей получения полезной информации из всей совокупности данных средств и систем обеспечения безопасности.

Снова об интеграции

Первой по назначению функцией систем класса PSIM является сбор данных от разнородных устройств, систем безопасности и прочих источников. Но о каких данных идет речь, например, в частном случае физической безопасности? Потратим некоторое количество слов, чтобы высветить проблематику, «спрятанную» за, казалось бы, «понятной» для всех темой – интеграцией. Для автоматизированного анализа, как и для традиционного мониторинга и управления, данные и прочая входящая информация должны быть приведены к некоторому единому словарю и смысловому полю, пространственным и временным координатам. Это относится как к событийным и параметрическим данным, так и к конфигурационным параметрам. Если системы сигнализации (тревоги, постановки/снятия с охраны…) имеют дело с дискретными событиями, то, например, в СКУД – это процессы, состоящие из последовательности событий, которые могут быть как «правильными», так и несущими информацию об отклонениях и нарушениях. Современные КСБ должны поддерживать и межсистемный информационный обмен. Наглядный пример: взаимодействие видеоподсистемы или VMS (система видеоменеджмента) с системами сигнализации, СКУД, технологического контроля и пр. С сожалением приходится констатировать, что, несмотря на десятилетия истории систем «класса PSIM», вопросы интеграции не стали менее значимы. В части видеоинформации ONVIF сделал много, и подключение типовых видеосервисов видеонаблюдения и видеозаписи все в большей степени становится рутинной задачей. Но минорные спецификации Profile C, A – это очень немного на фоне неинтероперабельных сервисов СКУД, а множество новых приложений и источников аналитических, биометрических данных и других средств и систем, которые необходимо интегрировать, только растет. Быстро растущий рынок источников данных для систем класса PSIM – Интернет вещей, который, к сожалению, характеризуется и нарастающим хаосом несовместимости.

В этих условиях большинство программных продуктов ССОИ, в том числе позиционируемых как PSIM, поддерживают/интегрируют лишь простые спецификации получения сигналов тревог и передачи команд. О каком-то анализе «больших данных» речь не идет в силу их отсутствия, что и ограничивает возможности систем инцидентным реагированием. Ситуация имеет и экономический подтекст. Поддержка «глубокой интеграции» неинтероперабельных средств и систем требует от разработчика наличия соответствующей зоны тестирования, широкой компетенции в области «чужих систем», поддержки и сопровождения не только своего, но и интегрируемых продуктов. Все это означает большие постоянные издержки и риски.

Большие данные

В комплексных системах безопасности и жизнеобеспечения присутствуют сотни и тысячи датчиков, извещателей, сенсоров и исполнительных устройств, которые генерируют миллиарды байт потенциально полезной информации. И только малая часть этих данных используется стандартными контроллерами и панелями в рамках традиционных процессов охраны.

Но предположим, что собираются все и любые данные, реализована глубокая интеграция. Допустим возможность применения известных технологий и инструментов Big Data для сбора, накопления, доступа к этим данным. Но и тогда отсутствие разработанных моделей получения полезной информации из полных потоков данных КСБ является основным тормозом реализации ключевого свойства PSIM, обозначенного в его имени – Information Management.

ВЫВОДЫ

Применительно к КСБ, PSIM – это новая концепция и новый класс программных средств ССОИ. PSIM отличают автоматизированный анализ полных потоков данных, автоматизация бизнес-процессов операторов и функции поддержки принятия решений. Ключевой принцип PSIM состоит во внедрении инструментов информационного менеджмента в деятельность служб безопасности.

Функции инцидентного управления и поддержки принятия решений легко встраиваются в существующие на рынке решения, а потому производители активно используют акроним PSIM в своих материалах. Судя по всему, легко произносимый акроним благодаря простоте и лаконичности английского технического языка оказался удачным маркетинговым инструментом.

Однако, главное в концепции PSIM – переход от практики узко инцидентного управления к настоящему информационному менеджменту. И на этом пути разработчикам систем класса PSIM придется столкнуться с двумя ключевыми проблемами. Сбор, накопление и автоматизированный анализ полных потоков данных КСБ, по всей видимости, невозможен без применения технологий больших данных. А для доступа к таким данным, прежде всего, необходима полнофункциональная интеграция. Качественная, «глубокая» интеграция средств, с поддержкой максимума их функциональных возможностей, является фундаментом реализации всех функций PSIM и при этом по-прежнему остается камнем преткновения.